Network Systems Use & Data Security Agreement

Introduction

Network systems and internet access are privileges available to employees and authorized non-employees ("System Users") of Galveston Independent School District ("District"). These services are intended to promote educational excellence within the district by facilitating communication, resource sharing, collaborative work, and innovation. The successful operation of the network depends on the proper conduct of System Users, who must adhere to strict guidelines. The following rules of acceptable use are provided to ensure System Users understand their ethical and legal responsibilities associated with the use of district network resources.

Scope

This Agreement ("Agreement") is between the district and system users who access or use district network systems, which include but are not limited to computers, application software, the Student Information System ("SIS"), finance data files, digitized information, removable media, servers, email, and internet services provided by the district.

Acceptable Use of Network Systems

System users should be aware that accessing internet content may expose them to material that may not have educational value within the school setting. The district has implemented precautions to limit access to controversial materials. However, due to the nature of the global network, it is impossible to control all content. While diligent users may encounter controversial information, the valuable resources and interactions available on this worldwide network outweigh the risk of accessing material inconsistent with District educational goals.

General Use:

Access to the District's electronic communications system is a privilege, not a right. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies.

- Use of district electronic communications systems is not confidential and is monitored 24 hours a day.
- There is no expectation of privacy, and all Internet activity is recorded.
- System users shall keep their passwords confidential.
- System users may not use another person's system account or email account.
- Attempts to log in to any computer network beyond the system user's authorized level of access may result in immediate cancellation of user privileges or other disciplinary action.
- System users may not allow students to access the network through their account.
- Any infraction of the Network Systems Use & Data Security Agreement by a system user shall be reported to the Director of MIS, MIS Network and Security Manager, and the MIS Technology & Cybersecurity Manager.
- The district, in its sole discretion, has the right to determine who is or is not given access to the district network and electronic communications systems.
- All digital content created for the district website or representing the district must adhere to the GISD Communications Department's web and branding standards.

Internet/Electronic Communications Use:

Access to the District's electronic communications system, including the Internet, is provided exclusively for instructional and administrative purposes and must strictly adhere to administrative regulations. Users should be aware that there is no expectation of privacy, and all Internet activity is subject to monitoring and recording.

System users are required to observe generally accepted rules of network etiquette (netiquette).

- Be polite and respectful: Treat others with courtesy and respect in all communications, whether in emails, chats, forums, or social media platforms.
- Use appropriate language: Avoid using offensive, discriminatory, or inflammatory language. Be mindful of cultural sensitivities and diverse perspectives.
- Respect privacy: Do not share personal information about yourself or others without permission. Respect confidentiality and data protection guidelines.
- Use appropriate formatting: Use clear and concise language. Avoid writing in all caps (which can be interpreted as shouting) or using excessive formatting (e.g., bright colors, large fonts) that may distract or annoy others.
- Be mindful of file attachments: Before sending file attachments, ensure they are relevant to the recipient and safe to open. Consider using cloud storage links instead of large attachments.
- Follow specific platform rules: Different online platforms may have their own rules and guidelines for usage. Familiarize yourself with these rules and adhere to them accordingly.

Computer Ethics:

- Accessing, copying, or transmitting any material that violates U.S. or state regulations is strictly prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene content, pornography, or material protected by trade secrets.
- Vandalism: Any malicious attempt to harm, modify, or destroy District equipment or materials, data belonging to another user of the district's system, or any agencies or networks connected to the Internet is strictly prohibited. Engaging in vandalism as described will result in the immediate cancellation of system use privileges and may require restitution for costs associated with system restoration, hardware, or software repairs.
- Deliberate attempts to degrade or disrupt system performance may constitute violations of District Policy and administrative procedures and could potentially be considered criminal activity under applicable state and federal laws. This includes, but is not limited to, uploading or creating computer viruses.

Restrictions:

- System users are prohibited from relocating or making modifications to district technology, including but not limited to computers, printers, and phones. Only MIS personnel are authorized to perform these changes and maintain an up-to-date inventory of all equipment and its locations.
- System users are strictly prohibited from installing personal or unauthorized computer equipment on the network. All devices connected to the network must be approved and provided by the district to ensure security and compliance with district policies.
- The use of VPNs or proxy services to establish independent data connections that bypass our network security mechanisms is strictly prohibited.
- Installation of software or other instruction resources must be conducted through appropriate channels and procedures. Software selection should adhere to the list of approved software provided by the District Instructional Technology Specialist.
- The MIS Department is responsible for retaining the original End User License Agreement ("EULA") and Data Protection Agreement ("DPA") for as long as the software or instructional resource are active.
- The use of district network resources for commercial activities or political lobbying is prohibited.

Student Data Security and Confidentiality

Employee and authorized non-employee use of district network systems and internet resources may involve access to restricted and/or confidential student data. It is crucial to recognize the need to protect students' personally identifiable information (PII) and other regulated data. This protection is required by district policy as well as state privacy laws and regulations, such as:

- The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (34 CFR Part 99)
- The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501-6506 (16 CFR Part 312)

General Use:

- System users must respect the confidentiality of student records and handle all student performance data, personally identifiable information (PII), and any other confidential or restricted data professionally.
- Follow all guidelines regarding the appropriate use of student data, whether collected by you or made available through other school district employees and associated systems. This includes, but is not limited to, the district's Student Information System (Skyward), Eduphoria, and any other files, applications, or online resources.
- System users must dispose of confidential reports in an appropriate manner when they are no longer needed.

Student Data Ethics:

- System users must comply with all relevant confidentiality laws, including district policies, state regulations, and federal laws such as the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99, as well as the Galveston ISD Student Data Confidentiality Agreement.
- Student data will only be accessed for students with whom system users have a legitimate educational interest and will be used solely to enhance student achievement.
- System users must securely log in and out of all resources that store student-specific data.
- Any documents containing student-specific data must be stored securely within the district network or in a password-protected environment.
- Regardless of its format, employees and authorized non-employees will treat all district data and information with the utmost respect for student privacy.

Restrictions:

- System users may not use another person's ID or password, nor share their own username and password.
- Ensure that data, including information on students, is not created, collected, stored, maintained, or disseminated in violation of district policy or state and federal data privacy laws.
- Uploading student data by system users to online resources is strictly prohibited.
- Confidential student-specific data must never be transmitted via email or as an email attachment unless the file is encrypted and/or password protected.
- It is illegal for a student to have access to another student's data and data from any source should not be shared by system users with any other student.
- System users will not share, store, or upload student-specific data on any personal computer or external devices that are not password protected. (external devices include but are not limited to USB/Thumb drives and external hard drives)
- System users will not leave student data, in any form, accessible or unattended, including information displayed on a computer screen.

I understand and agree to abide by the Galveston ISD Network Systems Use & Data Security Agreement. I further acknowledge that noncompliance with applicable rules and regulations may result in suspension or termination of network privileges and other disciplinary actions in accordance with District policies. Also, law violations may lead to criminal prosecution and disciplinary action by the district.

Revised: August 1, 2024